UNITED STATES DISTRICT COURT

DISTRICT OF PUERTO RICO

PABLO J. QUINTERO, and JOANNIE PRINCIPE, individually and on behalf of all others similarly situated, Plaintiffs, v. METRO SANTURCE, INC., d/b/a PAVIA HOSPITAL SANTURCE a corporation, METRO HATO REY, INC., d/b/a PAVIA HOSPITAL HATO REY and DOES 1 to 10, inclusive, Defendants.	CASE NO.: 20-1075 **CLASS ACTION** **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Pablo J. Quintero and Joannie Principe ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action based upon their personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigation of their attorneys.

NATURE OF THE ACTION

1. Defendant Metro Santurce, Inc. ("Metro Santurce") owns and operates the Pavia Hospital Santurce. Defendant Metro Hato Rey, Inc. ("Metro Hato Rey") owns and operates the Pavia Hospital Hato Rey (Metro Santurce and Metro Hato Rey are herein referred to as "Defendants"). Thousands of patients count on Metro Santurce and Metro Hato Rey to treat them competently and to handle their sensitive medical and personal information with care.

2. These patients reasonably expect the highest level of protection for their private identifiable information, when giving highly sensitive information such as their Social Security numbers and medical information to medical providers and insurers. What these patients do not expect, and did not expect, was that their personal and sensitive information would be harvested by unauthorized individuals.

3. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter, "Class Members"), bring this class action to secure redress against Defendants for

their reckless and negligent violation of patient privacy rights. Plaintiffs and Class Members are patients of Metro Santurce and Metro Hato Rey who were exposed by a data breach.

4. Plaintiffs and Class Members suffered significant injuries and damages. On information and belief, the security breach compromised the full names, addresses, dates of birth, gender, financial information, and social security numbers (referred to collectively as "PII")[1] of Plaintiffs and the Class Members.

5. As a result of Defendants' wrongful actions and inactions, unauthorized individuals gained access to and harvested Plaintiffs' and Class Members' PII. Plaintiffs have been forced to take remedial steps to protect themselves from future loss. Indeed, all Class Members are currently at a very high risk of identity theft and/or credit fraud, and prophylactic measures, such as the purchase of credit monitoring, are reasonable and necessary to prevent and mitigate future loss.

6. As a result of Defendants' wrongful actions and inactions, patient information was stolen. Many Metro Santurce and Metro Hato Rey patients have had their PII compromised, have had their privacy rights violated, have been exposed to the risk of fraud and identify theft, and have otherwise suffered damages.

7. Further, despite the fact that the breach was discovered on February 12, 2019, Defendants did not begin notifying their customers of the event until June 18, 2019, over four months later.

THE PARTIES

8. Plaintiff Pablo J. Quintero is a Puerto Rico citizen residing in Guaynabo, Puerto Rico. Plaintiff Quintero received medical care from Metro Santurce, pursuant to which Metro Santurce obtained Plaintiff Quintero's PII.

9. Plaintiff Joannie Principe is a Puerto Rico citizen residing in Carolina, Puerto Rico. Plaintiff Principe received medical care from Metro Hato Rey, pursuant to which Metro Hato Rey obtained Plaintiff Principe's PII.

10. Plaintiffs are informed and believe that, as a result of the data breaches that took

[1] The PII here referenced also constitutes PHI as defined by HIPAA.

place at Metro Santurce and Metro Hato Rey, Plaintiffs' PII was accessed by hackers. As a result, Plaintiffs have to purchase credit and personal identity monitoring services to alert them to potential misappropriation of their identity and to combat risk of further identity theft. At a minimum, therefore, Plaintiffs have suffered compensable damages because they will be forced to incur the cost of a monitoring service, which is a reasonable and necessary prophylactic step to prevent and mitigate future loss. Exposure of Plaintiffs' PII as a result of the data breach has placed them at imminent, immediate and continuing risk of further identity theft-related harm.

11. Defendant Metro Santurce is a corporation with its principal offices located in Guaynabo, Puerto Rico. Metro Santurce owns and operates the Pavia Hospital Santurce.

12. Defendant Metro Hato Rey is a corporation with its principal offices located in Guaynabo, Puerto Rico. Metro Hato Rey owns and operates the Pavia Hospital Hato Rey.

13. Plaintiffs are unaware of the true names, identities, and capacities of the defendants sued herein as DOES 1 to 10. Plaintiffs will seek leave to amend this complaint to allege the true names and capacities of DOES 1 to 10 if and when ascertained. Plaintiffs are informed and believe, and thereupon allege, that each of the defendants sued herein as a DOE is legally responsible in some manner for the events and happenings alleged herein and that each of the defendants sued herein as a DOE proximately caused injuries and damages to Plaintiffs and Class Members as set forth below.

14. As used herein, "Defendants" shall refer to Metro Santurce, Metro Hato Rey, and DOES 1 to 10, collectively.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over the claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), since some of the Class Members are citizens of a State different from the Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million.

16. The Court has personal jurisdiction over Defendants because Plaintiffs' and Class Members' claims arise out of Defendants' business activities conducted in Puerto Rico, where Defendants' headquarters are located.

17. Venue is appropriate in this District because, among other things: (a) Plaintiffs resides in this District, (b) Defendants maintain offices in this District, where they conduct substantial business; (c) Defendants directed their activities at residents in this District; and (d) many of the acts and omissions that give rise to this Action took place in this judicial District.

18. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because Defendants conduct a large amount of their business in this District, and because Defendants have substantial relationships in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

19. On February 12, 2019, the Pavia Hospital Santurce, owned and operated by Defendant Metro Santurce, and the Pavia Hospital Hato Rey, owned and operated by Defendant Metro Hato Rey, suffered a computer hack in which money was demanded in exchange for the release of the computer systems. During this hack, critical patient PII was exposed to the hackers.

20. On June 18, 2019, over four months later, Defendants began sending letters to the breach victims to inform them of the data breaches.

21. Defendants made repeated promises and representations to their patients, which formed a part of their contracts with those patients, that they would protect Plaintiffs' and the Class Members' PII from disclosure to third parties, including taking appropriate steps to safeguard their electronic databases. The Pavia Hospital Santurce's and Pavia Hospital Hato Rey's websites each contains a page titled "HIPAA Law," which states that each hospital "understands that the information on the patient's health is exclusively personal and we are committed to protecting the patient's privacy," and that "[a]ccording to the law we must . . . [m]ake sure to maintain the privacy of medical information that identifies you." (*See* Privacy Notices, translated on December 26, 2019, **Ex. A and B**). The Privacy Notices proceed to list the specific ways in which the hospitals are permitted to disclose PII, none of which were present in the current case, and state that no other disclosures will take place without written authorization.

22. Defendants promised that they would not disclose Plaintiffs' and the Class Members' PII to any unauthorized third parties. In fact, they allowed hackers to obtain it.

B. Defendants Had an Obligation to Protect Personal Information under Federal Law.

23. Defendants are entitles covered by HIPAA (*see* 54 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information").

24. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502. HIPAA also requires that Defendants implement appropriate safeguards for this information. 45 C.F.R. § 164.530(c)(1). HIPAA additionally requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable—i.e. non-encrypted data—to unauthorized third parties. 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

25. Additionally, HIPAA requires that Defendants:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);

(b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);

(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);

(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *see* 45 C.F.R. § 164.306(a)(3);

(e) Ensure compliance with the HIPAA security standard rules by its workforce, *see* 45 C.F.R. § 164.306(a)(4); and

(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

26. Defendants are additionally prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45, from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has found that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3d Cir. 2015). [2]

27. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

28. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[3] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. [4]

29. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers

---

[2] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 22, 2019).

[3] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 22, 2019).

[4] *Id*.

have implemented reasonable security measures. [5]

30. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations. [6]

31. In this case, Defendants were fully aware of their obligation to use reasonable measures to protect the personal information of their patients, acknowledging as much in their own privacy policies. Defendants also knew they were targets for hackers. But despite understanding the consequences of inadequate data security, Defendants failed to comply with industry-standard data security requirements.

32. Defendants failure to employ reasonable and appropriate measures to protect against unauthorized access to members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

C. Applicable Standards of Care

33. In addition to their obligations under federal law, Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel

[5] Federal Trade Commission, *Start With Security A Guide for Business* (Jun. 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 10, 2019).

[6] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Nov. 22, 2019).

responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

34. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

35. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

36. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to implement processes that would detect a breach of their data security systems in a timely manner.

37. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to act upon data security warnings and alerts in a timely fashion.

38. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendants' or to entrust PII with Defendants.

39. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose in a timely and accurate manner when data breaches occurred.

40. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants received the PII from other parties with the understanding that Plaintiffs and the Class Members expected their PII to be protected from disclosure. Defendants knew that a breach of the hospitals' data systems would cause Plaintiffs and the Class Members to incur damages.

D. Stolen Information Is Valuable to Hackers and Thieves

41. It is well known, and the subject of many media reports, that PII is highly coveted and a frequent target of hackers. According to a report by the HIPAA Journal, "healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published."[7] As reflected in the chart below, many of the largest healthcare breaches over the last decade have involved millions of patient or member records.

///

Largest Healthcare Data Breaches (2009-2018)

Rank	Name of Covered Entity	Year	Covered Entity Type	Individuals Affected	Type of Breach
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
3	Excellus Health Plan Inc.	2015	Health Plan	10,000,000	Hacking/IT Incident
4	Science Applications International Corporation	2011	Business Associate	4,900,000	Loss
5	University of California, Los Angeles Health	2015	Healthcare Provider	4,500,000	Hacking/IT Incident
6	Community Health Systems Professional Services Corporations	2014	Business Associate	4,500,000	Hacking/IT Incident
7	Advocate Medical Group	2013	Healthcare Provider	4,029,530	Theft
8	Medical Informatics Engineering	2015	Business Associate	3,900,000	Hacking/IT Incident
9	Banner Health	2016	Healthcare Provider	3,620,000	Hacking/IT Incident
10	Newkirk Products, Inc.	2016	Business Associate	3,466,120	Hacking/IT Incident

[7] Healthcare Data Breach Statistics, HIPAA JOURNAL, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Aug. 9, 2019).

42. Despite well-publicized litigation and frequent public announcements of data breaches, Defendants maintained an insufficient and inadequate system to protect the PII of Plaintiffs and Class Members.

43. Legitimate organizations and members of the criminal underground alike recognize the value of PII. Otherwise, they would not aggressively seek and pay for it. As previously seen in one of the world's largest data breaches, hackers compromised the card holder data of 40 million of Target's customers. *See* "Target: 40 million credit cards compromised," CNN Money, Dec. 19, 2013, *available* at http://money.cnn.com/2013/12/18/news/companies /target-credit-card/**.** DataCoup is, in contrast, just one example of a legitimate business that pays users for personal information. *See* http://money.com/money/3001361/datacoup-facebook-personal-data-privacy/.

44. PII is highly valuable to hackers. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII that is stolen from the point of sale are known as "dumps." *See* Krebs on Security April 16, 2016, Blog Post, *available at* https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/. PII can be used to clone a debit or credit card. *Id.*

45. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

46. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information,

including birthdates and Social Security numbers."[8]

E. The Data Breach Has Resulted and Will Result in Identity Theft and Identity Fraud

47. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiffs and Class Members.

48. The ramifications of Defendants' failure to keep Plaintiffs' and Class Members' PII secure is severe. According to Javelin Strategy and Research, "one in every three people who is notified of being a potential fraud victim becomes one . . . with 46% of consumers who had cards breached becoming fraud victims that same year." "Someone Became an Identity Theft Victim Every 2 Seconds Last Year," Fox Business, Feb. 5, 2014 *available* at http://www.foxbusiness.com/personal-finance/2014/02/05/someone-became-identitytheft-victim-every-2-seconds-last-year.html.

49. In the case of a data breach, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems." *See* "Victims of Identity Theft," U.S. Department of Justice, Dec 2013, *available at* https://www.bjs.gov/content/pub/pdf/vit12.pdf. In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*. at 11.

50. A person whose PII has been obtained and compromised may not know or experience the full extent of identity theft or fraud for years. It may take some time for the victim to become aware of the theft or fraud. In addition, a victim may not become aware of fraudulent charges when they are nominal, because typical fraud-prevention algorithms fail to capture such charges. Those charges may be repeated, over and over again, on a victim's account, without notice for years.

51. The damage from PII exposure is particularly acute in the medical context. A study by Experian found that the "average total cost" of medical identity theft is "about

[8] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf

$20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 a.m.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/. Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all. *Id*.

52. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Medical data is particularly valuable because unlike financial information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendants, are intended targets of cyber-criminals.

53. The Personal Information also has substantial legitimate value to Defendants. As Defendants' privacy policies recognize, they use Plaintiffs' Personal Information for business purposes other than administering claims. Many companies that retain Personal Information like that exposed in the data breach attribute inherent monetary value to it—even listing it as an asset on their books or using it as collateral or consideration for other transactions. Personal Information, including de-identified medical information, is a valuable commodity in the data-

driven market place and is often sold and traded between companies—subject to legal and contractual restrictions.

54. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple and discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases, and viewed and used by different criminal actors.

55. Exposure of this information to the wrong people can have serious consequences. The impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[9] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

56. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and

[9] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Nov. 22, 2019).

monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[10]

57. As a result of the data breach, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are also subject to a higher risk of phishing and pharming where hackers exploit information they already obtained in an effort to procure even more PII. Plaintiffs and Class Members are presently incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies. In addition, Plaintiffs and Class Members now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

F. Plaintiffs and Class Members Suffered Damages

58. The exposure of Plaintiffs' and Class Members' PII to unauthorized third-party hackers was a direct and proximate result of Defendants' failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by their contracts with Plaintiffs and the Class Members, and federal law. The data breach was also a result of Defendants' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII in order to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts and federal law

59. Plaintiffs' and Class Members' PII is private and sensitive in nature and was inadequately protected by Defendants. Defendants did not obtain Plaintiffs' and Class Members' consent to disclose their PII, except to certain persons not relevant to this action, as required by applicable law and industry standards.

60. As a direct and proximate result of Defendants' wrongful actions and inaction

[10] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Nov. 22, 2019).

and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

61. Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure, compromising, and theft of their PII;

b. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of unauthorized third-party hackers and misused via the sale of Plaintiffs' and Class Members' information on the Internet black market;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

62. Plaintiffs bring this action on their own behalf and on behalf of all others similarly situated under Rule 23(a), (b)(3), and (c)(4) of the Federal Rules of Civil Procedure. The Class is divided into two Classes as follows:

> The Puerto Rico Class:
>
> All persons residing in the Territory of Puerto Rico whose Personal Identifying Information was compromised as a result of the data breach of the Pavia Hospital Santurce and the Pavia Hospital Hato Rey, discovered on February 12, 2019.

The National Class:

> All persons residing in the United States whose Personal Identifying Information was compromised as a result of the data breach of the Pavia Hospital Santurce and the Pavia Hospital Hato Rey, discovered on February 12, 2019.

63. Excluded from the Class are: (a) Defendants, including any entity in which any of the Defendants has a controlling interest, is a parent or a subsidiary of, or which is controlled by any of the Defendants; (b) the officers, directors, and legal representatives of Defendants; and (c) the judge and the court personnel in this case as well as any members of their immediate families. Plaintiffs reserves the right to amend the definition of the Class if discovery, further investigation and/or rulings by the Court dictate that it should be modified.

64. *Numerosity*. The members of the Class are so numerous that the joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, given the number of patients who trust their care to Defendants, it stands to reason that the number of Class Members is in the thousands. Class Members are readily identifiable from information and records in Defendants' possession, custody, or control, such as account information.

65. *Commonality and Predominance*. There are questions of law and fact common to Class Members, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants owed a duty of care to Plaintiffs and Class Members with respect to the security of their PII;

b. What security measures must be implemented by Defendants to comply with their duty of care;

c. Whether Defendants met the duty of care owed to Plaintiffs and the Class Members with respect to the security of the PII;

d. Whether Defendants have a contractual obligation to Plaintiffs and Class Members to use reasonable security measures;

e. Whether Defendants have complied with any contractual obligation to use reasonable security measures;

f. What security measures must be implemented by Defendants to comply with their contractual obligations to use reasonable security measures;

g. Whether Defendants' acts and omissions described herein violated the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

h. Whether Defendants' acts and omissions described herein violated the Federal Trade Commission Act, 15 U.S.C. § 45;

i. What security measures, if any, must be implemented by Defendants to comply with their contractual and statutory obligations;

j. The nature of the relief, including equitable relief, to which Plaintiffs and Class Members are entitled; and

k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties and/or injunctive relief.

66. *Typicality*. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of each of the other Class Members, was exposed and/or improperly disclosed by Defendants.

67. *Adequacy of Representation*. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and Class Members have a unified and non-conflicting interest in pursuing the same claims and obtaining the same relief. Therefore, all Class Members will be fairly and adequately represented by Plaintiffs and their counsel.

68. *Superiority of Class Action*. A class action is superior to other available methods for the fair and efficient adjudication of the claims alleged in this action. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially

conflicting adjudications of the asserted claims. There will be no difficulty in the management of this action as a class action, and the disposition of the claims of the Class Members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied.

69. Class certification is also appropriate because Defendants have acted or refused to act on grounds generally applicable to the Class Members, such that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

FIRST CAUSE OF ACTION

(Breach of Express And/or Implied Contractual Promise)

70. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 69, inclusive, of this Complaint as if set forth fully herein.

71. Defendants were parties to contracts with Plaintiffs and the Class Members for medical services, pursuant to which Defendants obtained Plaintiffs' and the Class Members' PII.

72. As a part of these contracts, Defendants promised to maintain adequate safeguards to protect the PII from disclosure to unauthorized third parties, and also promised not to disclose the PII to unauthorized third parties. Defendants promised that "the information on the patient's health is exclusively personal and we are committed to protecting the patient's privacy," and that "[a]ccording to the law we must . . . [m]ake sure to maintain the privacy of medical information that identifies you." They also promised that "[a]ny other use or disclosure" of PII "that is not described in this Notice of Privacy Practice requires the patient's written authorization." **Ex. A and B**.

73. Accordingly, Defendants' promises to safeguard and protect the PII are contractually binding upon Defendants with regard to Plaintiffs and each of the Class members.

74. The contractual duty to protect and safeguard Plaintiffs' and the Class Members' PII, which Defendants promised to undertake, was, even apart from the language of the

contracts, a term of the contracts by operation of law under the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E., and under the Federal Trade Commission Act, 15 U.S.C. § 45. Under applicable common law, all laws in place at the time a contract is entered which are relevant to the subject matter of that contract become binding terms of the contract. Therefore, the HIPAA Privacy Rule and Security Rule, and the FTCA also formed a contractual term in each of Defendants' contracts with Plaintiffs and the Class Members.

75. Finally, the promise to safeguard and protect Plaintiffs' and the Class Members' PII, and keep that PII from being accessed by third parties, was implied as a matter of law because Defendants and Plaintiffs and the Class Members entered their agreements with the expectation and implied mutual understanding that Defendants would strictly maintain the confidentiality of the PII and safeguard it from theft or misuse.

76. Therefore, Plaintiffs and Class Members entered contracts for medical services with Defendants in which Defendants agreed to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' personal information from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

77. Plaintiffs and the Class Members would not have provided and entrusted the PII to Defendants in the absence of the proper security safeguards and the promise to keep their PII safe.

78. Plaintiffs and the Class Members fully performed their obligations under their agreements with Defendants.

79. Defendants breached the contractual promises by failing to: (a) implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) prevent unauthorized third parties from obtaining access to Plaintiffs' and Class Members' PII.

80. Plaintiffs' and the Class Members' expectation was that their PII would be safeguarded and protected. Therefore, they agreed to pricing terms to which they would not

have agreed had they known that their PII would not be protected. Further, due to the fact that their PII was not protected, Plaintiffs and the Class Members incurred losses associated with the loss of PII privacy, including theft, identity theft, and the risk of theft and identity theft, along with the necessity of cancelling credit cards and paying for additional protection through the market. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

81. As a direct and proximate result of Defendants' breaches of the contractual promises alleged herein, Plaintiffs and Class Members sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

(Breach of Covenant of Good Faith and Fair Dealing)

82. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 81, inclusive, of this Complaint as if set forth fully herein.

83. Applicable law implies a covenant of good faith and fair dealing in every contract.

84. Plaintiffs and Class Members entered contracts with Defendants for medical services.

85. Plaintiffs and the Class Members performed all of their duties under their agreements with Defendants.

86. All of the conditions required for Defendants' performance under the contracts have occurred.

87. Incorporated in the contracts as a matter of law was the covenant of good faith and fair dealing, which prevents a contracting party from engaging in conduct that frustrates the other party's rights to the benefits of the agreement. The implied covenant imposes on a contracting party not only the duty to refrain from acting in a manner that frustrates performance of the contract, but also the duty to do everything that the contract presupposes that the contracting party will do to accomplish its purposes.

88. Here the implied covenant of good faith and fair dealing required Defendants, under the terms of their agreement which stated that Defendants would protect the PII, to safeguard and protect from disclosure to third parties the PII of Plaintiffs and the Class Members which was turned over to Defendants only for the purposes of performing medical services. Plaintiffs and the Class Members could not enjoy Defendants' services without the safeguarding and protection of the PII.

89. Defendants breached the covenant of good faith and fair dealing implied in their contracts by engaging in the following conscious and deliberate acts: (a) failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure; and (b) failing to ensure that unauthorized parties were not provided access to Plaintiffs' and Class Members' PII. Defendants' failure to protect the PII of Plaintiffs and Class Members frustrated Plaintiffs' and the Class Members' rights to the benefit of their bargains with Defendant, to enjoy the professional services of Defendant without incurring risks of property and identity theft.

90. Plaintiffs and Class Members have lost the benefit of their contracts by having their PII compromised and have been placed at an imminent, immediate and continuing risk of identity theft-related harm. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

91. As a direct and proximate result of Defendants' breach of the covenant of good faith and fair dealing, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

(Negligence)

92. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 91, inclusive, of this Complaint as if set forth fully herein.

93. As described above, Defendants owed Plaintiffs and the Class Members duties of care in the handling of PII, which duties included keeping that PII safe and preventing

disclosure of that PII to all unauthorized third parties.

94. Additionally, Defendants owed a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' PII as required by HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E, and Federal Trade Commission Act, 15 U.S.C. § 45. This legal duty arises outside of any contractual, implied or express, responsibilities that Defendants had between Plaintiffs and Class Members, as it is completely independent of any contract.

95. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information." 45 C.F.R. § 164.502. HIPAA also requires that Defendants implement appropriate safeguards for this information. 45 C.F.R. § 164.530(c)(1). HIPAA additionally requires that Defendants provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable—i.e. non-encrypted data—to unauthorized third parties. 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

96. Additionally, HIPAA requires that Defendants:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights, *see* 45 C.F.R. § 164.312(a)(1);
(b) Implement policies and procedures to prevent, detect, contain, and correct security violations, *see* 45 C.F.R. § 164.306(a)(1);
(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, *see* 45 C.F.R. § 164.306(a)(2);
(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, *see* 45 C.F.R. § 164.306(a)(3);
(e) Ensure compliance with the HIPAA security standard rules by its workforce, *see* 45 C.F.R. § 164.306(a)(4); and
(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. § 164.530(b).

97. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

98. Defendants violated the above listed regulations by disclosing the PII to third

parties and by failing to implement adequate security measures to protect the PII, including failing to:

(a) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;
(b) Implement policies and procedures to prevent, detect, contain, and correct security violations;
(c) Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;
(d) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;
(e) Ensure compliance with the HIPAA security standard rules by its workforce; and
(f) Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information.

99. Defendants also violated §§ 164.404 and 164.402 by failing to provide timely notice of the breach to Plaintiffs and the Class Members.

100. The harm that occurred as a result of the security breach is the type of harm that HIPAA was intended to guard against. HIPAA directly requires subject entities to protect the health information of individuals such as Plaintiffs and the Class Members.

101. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

102. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

103. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a company as large as Defendants', including, specifically, the damages that would result to

Plaintiffs and Class members.

104. The harm that occurred as a result of the security breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

105. Defendants' failure to comply with applicable laws and regulations constitutes negligence per se.

106. In addition to their obligations under state and federal law, Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems and networks, and the personnel responsible for them, adequately protected the PII of Plaintiffs and the Class Members.

107. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to design, maintain, and test their computer system to ensure that the PII in Defendants' possession was adequately secured and protected.

108. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to create and implement reasonable data security practices and procedures to protect the PII in their possession, including adequately training their employees and others who accessed PII within their computer systems on how to adequately protect PII.

109. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to implement processes that would detect a breach of their data security systems in a timely manner.

110. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted

them with sensitive PII, to act upon data security warnings and alerts in a timely fashion.

111. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to purchase insurance or other health care services from Defendants' or to entrust PII with Defendants.

112. Defendants owed a duty to Plaintiffs and the Class Members, who entrusted them with sensitive PII, to disclose in a timely and accurate manner when data breaches occurred.

113. Defendants owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendants collected Plaintiffs' and the Class Members' PII. Defendants knew that a breach of their data systems would cause Plaintiffs and the Class Members to incur damages.

114. Defendants breached those duties of care by adopting inadequate safeguards to protect the PII, and, on information and belief, failing to adopt industry-wide standards in their supposed protection of the PII, resulting in the disclosure of the PII to unauthorized third parties.

115. As a direct and proximate result of Defendants' failure to adequately protect and safeguard the PII, Plaintiffs and the Class members suffered damages. Plaintiffs and the Class Members were damaged because their PII was accessed by third parties, resulting in increased risk of identity theft and theft of property, and for which Plaintiffs and the Class members were forced to adopt costly and time-consuming preventive and remediating efforts. Plaintiffs and the Class Members were also damaged in that they paid for services in an amount that they would have refused to pay had they known that Defendants would not protect their PII. Plaintiffs and the Class Members accepted pricing terms which they would not have agreed to had they known that Defendants would not protect their PII. The risk of identity theft which Plaintiffs now faces is considerable. Hackers do not target PII without the intent to use it fraudulently.

116. Defendants acted with wanton disregard for the security of Plaintiffs' and the Class Members' PII. Defendants knew or should have known that Defendants had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the PII of health care providers' databases, such as Defendants'.

117. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiffs and the Class Members to experience the foreseeable harm associated with the exposure of their PII.

118. A "special relationship" exists between Defendants and Plaintiffs and the Class Members. Defendants entered into a "special relationship" with Plaintiffs and the Class Members when they contracted with Plaintiffs' and the Class Members to provide them with medical care and obtained Plaintiffs' and the Class Members' PII from them. As providers of health care services, Defendants stand in a fiduciary or quasi-fiduciary relationship with Plaintiffs and the Class Members.

119. Plaintiffs and the Class Members have suffered monetary injury in fact as a direct and proximate result of the acts committed by Defendants as alleged herein in an amount to be proven at trial but in excess of the minimum jurisdictional amount of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for relief as follows:

1. For compensatory damages in an amount according to proof at trial;

2. For affirmative injunctive relief mandating that Defendants implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Class Members' PII from unauthorized access, destruction, use, modification, or disclosure;

3. For costs of suit and litigation expenses;

4. For attorneys' fees under the common fund doctrine and all other applicable law;

and

5. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

Dated: February 11, 2020

Respectfully submitted,

/s/ *David C. Indiano*
David C. Indiano USDC Bar No. 200601
Jeffrey M. Williams USDC Bar No. 202414
Vanesa Vicéns-Sánchez USDC Bar No. 217807
Christopher A. Dávila USDC Bar No. 304103
INDIANO & WILLIAMS, P.S.C.
207 del Parque Street, Third Floor
San Juan, Puerto Rico 00912
Telephone: (787) 641-4545
Facsimile: (787) 641-4544

/s/ *Thiago M. Coelho*
Bobby Saadian*
Justin F. Marquez*
Thiago M. Coelho*
Robert J. Dart*
WILSHIRE LAW FIRM
3055 Wilshire Blvd., 12th Floor
Los Angeles, California 90010
Telephone: (213) 381-9988
Facsimile: (213) 381-9989

(**pro hac vice applications forthcoming*)

Attorneys for Plaintiffs and the Proposed Class